	Application No.	Applicant(s)	
Office Action Summary	10/656,439	SMETTERS ET AL.	
	Examiner	**Art Unit**	
	Samson B. Lemma	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 February 2008*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-4,6-13,15-22 and 24-30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4, 6-13,15-22 and 24-30* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *01/22/08*.

4) ☒ Interview Summary (PTO-413)
Paper No(s)/Mail Date. *held on 01/10/08* .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. This office action is in reply to an amendment filed on February 13, 2008. **Claims 5, 14 and 23** have previously been canceled. Thus claims 1-4, 6-13, 15-22 and 24-30 are pending of which claims 1, 10 and 19 are independent claims. Each and every independent claim is amended.

2. Applicant's representative and Examiner have conducted a telephone interview on January 10/2008. The summary of the interview has been attached.

Priority

3. This application claims priority of a provisional application 60/480,909 filed on June 24, 2003. Therefore, the effective filling data for the subject matter defined in the pending claims of this application is **06/24/2003.**

Response to Arguments

4. Applicant's argument/s filed on February 13, 2008 have been fully considered but they are not persuasive.

Applicant's representative argued that the following new limitation which is added to the respective independent claims, "**prior to establishing the communication, pre-authenticating the**

situation notification device to ensure that the situation notification device has physical access to the preferred channel" is not disclosed by the reference/s on the record.

Applicant's representative wrote the following in support of his argument.

"Pre-authenticating the situation notification device allows an administrator of the preferred channel to be assured that during communication, credentials (such as keys) can only be provided to the trusted member devices. More specifically, such a trust on a member device is established based on the physical access to the preferred channel. For example, if the user is an employee who has physical access to the building where the preferred channel is located, the user can be trusted to communicate and receive credentials over the preferred channel.

There is nothing within ***Hermann and Stirbu,*** *either separately or in concert, which suggests pre-authenticating a device to ensure that the device has physical access to a preferred channel, before establishing the communication between the situation notification device and the provisioning device over a preferred channel."*

Examiner disagrees with this argument.

The Examiner disagreement is based on the fact that the limitation which is argued is something which is already disclosed by the primary reference on the record.

Examiner in particular would like to point out that Hermann, the primary reference on the record on paragraph 0021-0022, discloses the following which meets the limitation "prior to establishing the communication, pre-authenticating the situation notification device to ensure that the situation notification device has physical access to the preferred channel"

" *[0021] For establishing an* ***authenticated session between the user's personal device and the serving device,*** *e.g. a bank terminal, the user points with the personal device to the serving device or at least in this direction and passes via a unidirectional wireless communication channel, e.g. via an infrared channel, a sequence or an initial-sequence that comprises* ***a password, a public key, a session key, identification parameters, and/or communication parameters.*** *After receiving the sequence, the serving device responds by sending back over a wireless broadcast medium encrypted information which can only be decrypted and used by the personal device.* ***The respond may comprise information, a key, also a session key, and communication parameters from the serving device for further***

communication over the wireless broadcast medium. The personal device receives the encrypted information.

[0022] For a secure session over the wireless broadcast medium keys are exchanged. ***Thus, an encrypted communication over the wireless broadcast medium can take place."***

This implies the fact that prior to an encrypted communication between the situation notification device/first device/user's personal device and the servicing device the notification device/first device/user's personal device is pre-authenticated.

In order to show how each and every limitation of the independent claims are disclosed by the reference/s on the record the examiner would show the following.

5. **As per independent claims 1, 10 and 19 Hermann discloses a computer controlled method comprising:**

- **Establishing communication between a situation notification device** [see , paragraph 0020, "first device"] **and a provisioning device** [see , paragraph 0020, "second device/servicing device"**] over a preferred channel [**See, paragraph 0020, "communication link"**];**[paragraph 0020, lines 15-21]

- **Prior to establishing the communication, pre-authenticating the situation notification device to ensure that the situation notification device has physical access to the preferred channel.** *[Paragraph 0021-0022] (On paragraph 0021, the following has been disclosed. "For establishing an* ***authenticated session between the user's personal device and the serving device,*** *e.g. a bank terminal, the user points with the personal device to the serving device or at least in this direction and passes via a unidirectional wireless communication channel, e.g. via an infrared channel, a sequence or an initial-sequence that comprises* ***a password, a public key, a session key, identification parameters, and/or communication parameters.*** *After receiving the sequence, the serving device responds by sending back over a wireless broadcast medium encrypted information which can only be decrypted and used by the personal device.* ***The respond may comprise information, a key, also a session key, and communication parameters from the serving device for further communication over the wireless broadcast medium. The personal device receives the encrypted information." Furthermore on paragraph 0022, the following has also been disclosed.*** *"For a secure session over the wireless broadcast medium keys are exchanged.* ***Thus, an encrypted communication over the wireless broadcast***

medium can take place." *This implies the fact that prior to an encrypted communication between the situation notification device/first device/user's personal device and the servicing device the notification device/first device/user's personal device is pre-authenticated.)*

- **Providing provisioning information to said situation notification device over said preferred channel,[Paragraph 0020, lines 44-48]** *(After receiving the sequence, the serving device responds by sending back over a wireless broadcast medium a respond. And as it is disclosed on paragraph 0020, lines 44-48 such responds may comprises, a key, also a session key and a communication parameters which meets the limitation of provisioning information from serving device to personal device/situation notification for further communication. In other words the personal device/situation notification device is provided with key, session key and a communication parameters/provisioning information)*

wherein said situation notification device is automatically configured to receive subject matter information responsive to said provisioning information; *[Paragraph 0020, lines 48-49] (And* *the situation notification device is automatically configured to receive the encrypted information which meets the limitation of the subject matter information)*

- **Receiving said subject matter information;** [Paragraph 0020, lines 48-49] (encrypted information)

- **Verifying said subject matter information with said provisioning information; [**Paragraph 0014**]** *(Only the intended receiver/notification device receives the encrypted subject matter since it is the one that has the corresponding decryption key and the encrypted information/subject matter information with the corresponding private key/public key/session key/provisioning information are decrypted and verified that the subject matter is sent form the right provisioning device.)*

- **Presenting said subject matter information to a user of the situation notification device responsive to the step of verifying, wherein the step of verifying ensures that the subject matter information is genuine.. [**Paragraph 0014 & abstract] *(Only the intended receiver/notification device receives the encrypted subject matter since it is the one that has the corresponding decryption key. And the encrypted* *information/subject matter information is presented to a user of the situation notification device only and only if the situation notification device carries the corresponding private key/public key/session key/provisioning information and successfully decrypts and verifies that the subject matter is sent form the right provisioning device, by doing so the situation notification device ensures that the subject matter information is genuine. This is simply another application of public key cryptograph, explained on paragraph 0014 and secure transmission disclosed in the abstract.)*

Hermann does not explicitly disclose the limitation recited as **"wherein the preferred channel does not require being resistant to eavesdropping."**

However, in the same field of endeavor **Stirbu on paragraph 0008**, discloses that a TLS Handshake Protocol allows a server and client in a communication session to authenticate each other and to negotiate an encryption algorithm and cryptographic keys before the application protocol transmits or receives its first byte of data. The TLS Handshake Protocol provides connection security having three basic properties: the peer's identity can be authenticated using asymmetric, or public key, cryptography (e.g., RSA, DSS, etc.); the negotiation of a shared secret is secure in that the **negotiated secret is unavailable to eavesdroppers,** and for any authenticated connection **the secret cannot be obtained,** even by an attacker who can place himself in the middle of the connection; **and the negotiation is reliable in that no attacker can modify the negotiation communication without being detected by the parties to the communication.**

Therefore all the elements of the limitations recited in the submitted amended claims are suggested/disclosed by reference/s on the record and the rejection remains valid.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. **Claims 1-4, 6-13, 15-22 and 24-30** are rejected under 35 U.S.C. 103(a) unpatentable over **Hermann, Reto** (hereinafter refereed as

Hermann) (European Patent Publication No. EP1024626A1) (Publication Date 08/02/2000) (Submitted with the Applicant's IDS) in view of Stirbu (hereinafter referred as **Stirbu)** (U.S. Publication No. 2003/0200431) (filed on: April 18, 2002)

8. **As per independent claims 1, 10 and 19 Hermann discloses a computer controlled method comprising:**

- **Establishing communication between a situation notification device [**see , paragraph 0020, "first device"] **and a provisioning device [**see , paragraph 0020, "second device/servicing device"**] over a preferred channel [**See, paragraph 0020, "communication link"**];**[paragraph 0020, lines 15-21]

- **Prior to establishing the communication, pre-authenticating the situation notification device to ensure that the situation notification device has physical access to the preferred channel.** *[Paragraph 0021-0022] (On paragraph 0021, the following has been disclosed. "For establishing an* ***authenticated session between the user's personal device and the serving device,*** *e.g. a bank terminal, the user points with the personal device to the serving device or at least in this direction and passes via a unidirectional wireless communication channel, e.g. via* *an infrared channel, a sequence or an initial-sequence that comprises* ***a password, a public key, a session key, identification parameters, and/or communication parameters.*** *After receiving the sequence, the serving device responds by sending back over a wireless broadcast medium encrypted information which can only be decrypted and used by the personal device.* ***The respond may comprise information, a key, also a session key, and communication parameters from the serving device for further communication over the wireless broadcast medium. The personal device receives the encrypted information." Furthermore on paragraph 0022, the following has also been disclosed.*** *"For a secure session over the wireless broadcast medium keys are exchanged.* ***Thus, an encrypted communication over the wireless broadcast medium can take place."*** *This implies the fact that prior to an encrypted communication between the situation notification device/first device/user's personal device and the servicing device the notification device/first device/user's personal device is pre-authenticated.)*

- **Providing provisioning information to said situation notification device over said preferred channel,[Paragraph 0020, lines 44-48]** *(After receiving the sequence, the serving device* *responds by sending back over a wireless broadcast medium a respond. And as it is disclosed on paragraph 0020, lines 44-48 such responds may comprises, a key, also a session key and a communication parameters which meets the limitation of provisioning information from serving device to personal device/situation notification for further communication. In other words the personal device/situation notification device is provided with key, session key and a communication parameters/provisioning information)*

Wherein said situation notification device is automatically configured to receive subject matter information responsive to said provisioning information; *[Paragraph 0020, lines 48-49] (And the situation notification device is automatically configured to receive the encrypted information which meets the limitation of the subject matter information)*

- **Receiving said subject matter information;** [Paragraph 0020, lines 48-49] (encrypted information)
- **Verifying said subject matter information with said provisioning information; [**Paragraph 0014**]** *(Only the intended receiver/notification device receives the encrypted subject matter since it is the one that has the corresponding*

decryption key and the encrypted information/subject matter information with the corresponding private key/public key/session key/provisioning information are decrypted and verified that the subject matter is sent form the right provisioning device.)

- **Presenting said subject matter information to a user of the situation notification device responsive to the step of verifying, wherein the step of verifying ensures that the subject matter information is genuine.. [**Paragraph 0014 & abstract] *(Only the intended receiver/notification device receives the encrypted subject matter since it is the one that has the corresponding decryption key. And the encrypted information/subject matter information is presented to a user of the situation notification device only and only if the situation notification device carries the corresponding private key/public key/session key/provisioning information and successfully decrypts and verifies that the subject matter is sent form the right provisioning device, by doing so the situation notification device ensures that the subject matter information is genuine. This is simply another application of public key cryptograph, explained on paragraph 0014 and secure transmission disclosed in the abstract.)*

> **Hermann does not** explicitly disclose the limitation recited as "**wherein the preferred channel does not require being resistant to eavesdropping.**"
>
> However, in the same field of endeavor **Stirbu on paragraph 0008**, discloses that a TLS Handshake Protocol allows a server and client in a communication session to authenticate each other and to negotiate an encryption algorithm and cryptographic keys before the application protocol transmits or receives its first byte of data. The TLS Handshake Protocol provides connection security having three basic properties: the peer's identity can be authenticated using asymmetric, or public key, cryptography (e.g., RSA, DSS, etc.); the negotiation of a shared secret is secure in that the **negotiated secret is unavailable to eavesdroppers,** and for any authenticated connection **the secret cannot be obtained,** even by an attacker who can place himself in the middle of the connection; **and the negotiation is reliable in that no attacker can modify the negotiation communication without being detected by the parties to the communication.**

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine the feature of which a channel does not need to be resistant to eavesdroppers to be used as a preferred channel because only public information (e.g., a public key, or a commitment to a public key) is sent over that channel; a pair of devices authenticating themselves to each other by sending such key or commitment information over the preferred channel are able to set up a secure communication with each other because they can demonstrate possession of the private keys corresponding to the public keys and eavesdropper that detects the commitment or keys sent across the preferred channel is not able to demonstrate possession of the corresponding private key as per teachings of **Stirbu** in to the method as taught **Hermann** in order to build a trust infrastructures. [See Stirbu, paragraph 0003]

9. <u>**As per claims 2, 11 and 20 the combination of**</u> **Hermann and Stirbu discloses a computer controlled method as applied to claims above. Furthermore, Hermann discloses a method, wherein the step of providing further comprises:**

exchanging key commitment information over said preferred channel between said provisioning device and said situation notification device; [paragraph 0020]

receiving a public key by said situation notification device; [paragraph 0021, line 39] **verifying said public key with said key commitment information** [Paragraph 0021, lines 41-42] **[**the serving device, inherently verifies the password or the public key sent by the personal device before responding to the personal device. After verification, the service device sends back a communication parameters for further communication to the personal device]**; and receiving a credential authorized by a credential issuing authority.** [paragraph 0022]

10. **<u>As per claims 3, 12 and 21 the combination of</u> Hermann and Stirbu discloses a computer controlled method as applied to claims above. Furthermore, Hermann discloses a method, wherein said preferred channel is a location-limited channel.** [paragraph 0020, lines 20-21]

11. **<u>As per claims 4, 13 and 22 the combination of</u> Hermann and Stirbu discloses a computer controlled method as applied to claims above. Furthermore, Hermann discloses a method, wherein, wherein said preferred channel uses a telephone switching system.** [paragraph 0025-0026 and 0041-0042]

12. **<u>As per claims 6, 15 and 24 the combination of</u> Hermann and Stirbu discloses a computer controlled method as applied to**

claims above. Furthermore, Hermann discloses a method, wherein subject matter information is received using an antenna, a telephone line, a local area network, a wide area network, a wireless network, or a broadcast network. [paragraph 0041-0042]

13. **As per claims 7, 16 and 25 the combination of Hermann and Stirbu discloses a computer controlled method as applied to claims above. Furthermore, Hermann discloses a method, wherein said situation notification device is a computer, a television, a radio, a telephone, a push to talk device, a pager, a clock, a thermostat, a network appliance, or a home appliance.** [paragraph 0039]

14. **As per claims 8-9, 17-18 and 26-27 the combination of Hermann and Stirbu discloses a computer controlled method as applied to claims above. Furthermore, Hermann discloses a method, further comprising forwarding said subject matter information, wherein said subject matter information is alarm information**. [Paragraph 0039, lines 44-46]

15. **As per claims 28-30 the combination of Hermann and Stirbu discloses a computer controlled method as applied to claims above. Furthermore, Hermann discloses a method, wherein said preferred channel has a demonstrative identification**

property and an authenticity property. [paragraph 0027] *(The limitation recited in the amended indepenent claims as the preferred channel has "demonstrative identification property" is defined as follows in applicant's specification, (see publication no. 20040268119, paragraph 0054, the last sentence), "The demonstrative identification property of the preferred channel means that human operators are aware of which devices are communicating with each other over the preferred channel and that the human operators can easily detect when an attack is being made on the preferred channel."*

Furthermore, the limitation recited in the amended indepenent claims as the preferred channel has "an authenticity property" is defined as follows in applicant's specification, (see publication no. 20040268119, paragraph 0055)

"The authenticity property of the preferred channel means that it is impossible or difficult for an attacker to transmit over the preferred channel or tamper with messages sent over the preferred channel without detection by the legitimate parties to the communication."

Examiner would like to point out that the reference on the record, namely Hermann discloses such concepts/limitation as shown below which meets the recitation the amended limitation.

Hermann on pargaraph 0026 discloses that initiating the communication session and for transmitting an initial-sequence that *may contain sensitive information, the unidirectional wireless communication channel can ensure that only the target deivice receives the initial-sequence. It is especially advantageous if a directed channel as line-of-sight link can be used, because than no other parties can eavesdrop and receive the initial-sequence. Such a channel can be an optical channel, e.g. an infrared or a laser channel, a Personal Area Network (PAN) channel, a directed radio-frequency (RF) channel, an inductive channel, a capacitive channel, or every other channel that is suitable for low-range, directed communication links.*

Furthermore Hermann on pargarph 0029, discloses that it is very simple to set up a communication if the personal device is connected to a user, e.g. by a PAN, because the user touches then in an intuitive way the serving device for initiating the unidirectional wireless communication channel via his body. There are no additional cards or other things necessary for setting up an authenticated session.

The above paragraphs such as paragraph 0026 & 0029 recited on the record implies the fact that "when attack is being made on the preferred channel it can easily detected"and meets the limitation recited as " the preferred channel has "demonstrative identification property" Likewise, Hermann on paragraph 0030, discloses that if the response as well as the further communication over the wireless *broadcast medium is protected by using a cryptosystem, than the advantage occurs, that the exchanged information is hidden perfectly and can not be uncovered by someone else. A suitable system can be a public-key cryptosystem where only the public key is exchanged once. Furthermore, what is recited on paragraph 0026 in combination with the "authenticated session" or "protected by using a cryptosystem" disclosed on paragraph 0026 and 0029, meets the limitation that "the preferred channel has "an authenticity property". Furthermore, Stirbu on paragraph 0008, discloses that a TLS Handshake Protocol allows a server and client in a communication session to authenticate each other and to negotiate an encryption algorithm and cryptographic keys before the application protocol transmits or receives its first byte of data. The TLS Handshake Protocol provides connection security having three basic properties: the peer's identity can be authenticated using asymmetric, or public key, cryptography (e.g., RSA, DSS, etc.); the negotiation of a shared secret is secure in that the negotiated secret is unavailable to eavesdroppers, and for any authenticated connection the secret cannot be obtained, even by an attacker who can place himself in the middle of the connection; and the negotiation is reliable in that no attacker can modify the negotiation communication without being detected by the parties to the communication.)*

Conclusion

16. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Samson B Lemma whose telephone number is 571-272-3806. The examiner can normally be reached on Monday-Friday (8:00 am---4: 30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, BARRON JR GILBERTO can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR.

/Samson B Lemma/
Examiner, Art Unit 2132
05/01/2008

/Gilberto Barron Jr/
Supervisory Patent Examiner, Art Unit 2132